Continuous Compliance

Enhancing Cybersecurity for Critical Infrastructure by Strengthening Regulation, Oversight, and Monitoring

Julian Baker
Continuous Compliance

Enhancing Cybersecurity for Critical Infrastructure by Strengthening Regulation, Oversight, and Monitoring

Julian Baker
About the Author

Julian Baker is a Master in Public Policy (MPP) candidate at Harvard University’s John F. Kennedy School of Government. His concentration is in international and global affairs, and he works as a research assistant for the Belfer Center’s Cyber Project. Julian previously served in the U.S. Army and worked in the research office of the Texas Senate. He graduated cum laude from Tulane University, where he received a bachelor’s in political science and spent time in Morocco and Spain.

About the Cyber Project

Forty years ago, an interdisciplinary group of Harvard scholars – professors, researchers and practitioners – came together to tackle the greatest threat of the Cold War: the fear of a nuclear exchange between the Soviet Union and the United States. Today, we seek to recreate that interdisciplinary approach to tackle a new threat: the risk of conflict in cyberspace. The problems that confront today’s leaders are substantial and diverse: how to protect a nation’s most critical infrastructure from cyberattack; how to organize, train, and equip a military force to prevail in the event of future conflict in cyberspace; how to deter nation-state and terrorist adversaries from conducting attacks in cyberspace; how to control escalation in the event of a conflict in cyberspace; and how to leverage legal and policy instruments to reduce the national attack surface without stifling innovation. These are just a sample of the motivating questions that drive our work. The aim of the Belfer Center’s Cyber Project is to become the premier home for rigorous and policy-relevant study of these and related questions.
Acknowledgments

The author thanks Anand Datla, Juliette Kayyem, Serena Larson, Bruce Schneier, and Nick Sinai for their contributions to this work. Their knowledge, guidance, and expertise provided the foundation for the research of this project. He also extends a special thank you to Lauren Zabierek, whose knowledge and effort helped guide this research throughout the process.

This student research was supported by funding from Amazon Web Services (AWS). The Cyber Project appreciates AWS support of student work in cyber-related issues.
# Table of Contents

**Executive Summary** ............................................................................................................. 1

**Critical Infrastructure Regulations in the United States** ............................................. 3

**Critical Infrastructure Cybersecurity Regulations Outside of the United States** ............................................................................................................. 7

**Point-in-time: Compliance in Practice** .................................................................................. 9

**Continuous Compliance: A More Effective Solution** ..................................................... 11

  - How Continuous Compliance Works ............................................................................ 15

**Recommendations** .................................................................................................................. 20

  - Government .................................................................................................................... 20

  - Critical Infrastructure Operators .................................................................................. 23

  - Continuous Compliance Software Providers .................................................................. 24

**Conclusion** ............................................................................................................................ 26
The U.S. Homeland Security Department headquarters in northwest Washington is pictured on Feb. 25, 2015. A popular Chinese-made automotive GPS tracker used by individuals, government agencies and companies in 169 countries has severe software vulnerabilities, posing a potential danger to life and limb, national security and supply chains, cybersecurity researchers said in a report released Tuesday, July 19, 2022, to coincide with an advisory from the U.S. Cybersecurity and Infrastructure Security Agency listing six vulnerabilities. (AP Photo/Manuel Balce Ceneta, File)
Executive Summary

An intrusion into a critical infrastructure facility risks the health, wellbeing, and safety of millions of people. The sixteen critical infrastructure sectors in the United States have little to no cybersecurity regulations or requirements. Cybersecurity standards, except for the energy, nuclear, and financial sectors, are voluntary and there is no legal penalty for lax practices. International standards are much the same: not mandatory and unenforceable.

Businesses that institute their own cybersecurity practices—even if they are stringent—often conduct an assessment or are audited on a point-in-time or period-in-time basis. This means that they verify adherence to a voluntary standard at a certain moment in time rather than in an ongoing manner. By assessing on a point-in-time basis, a business can only determine that they comply at that moment, rather than being notified when networks are noncompliant or drifting away from compliance standards or best practices.

Furthermore, many companies that run U.S. critical infrastructure are small, rural, or underfunded. These facilities do not have the financial resources to upgrade their cybersecurity practices and ensure ongoing monitoring, making them attractive targets to threat actors. They are poorly defended yet still responsible for facilities serving large populations. Recent intrusions, including ransomware and other attacks, have demonstrated the ease with which motivated threat actors can access these networks.

A transition from a point-in-time framework to a method of continuous compliance would raise the level of cybersecurity for critical infrastructure, making these essential services more reliable for the people relying on them. Continuous compliance represents a security posture and set of operational practices where an organization can persistently monitor, identify, and rectify current or potential lapses in their cybersecurity to ensure adherence to legal standards and industry best practices. The transition to continuous compliance requires a shift in an organization’s
mindset to embrace monitoring, evaluation, learning, and adapting in an ongoing manner. It also requires enabling technologies, such as artificial intelligence and a compliance engine, which is software and a service that monitors specified inputs to measure compliance, track progress, and identify noncompliant systems and behaviors.

For businesses looking to make this transition, administrators must define and regulate cybersecurity standards, create methods to measure noncompliance and drift, and establish systems for notification of noncompliance within the network. Some of the services that a compliance engine can provide include alerting an administrator of risks to the network like employees not using multi-factor authentication, still active accounts of former employees, or third-party access credentials still in use after a contract terminates. The main benefits of continuous compliance are increased cybersecurity for the business, increased reliability for the public, and decreased cost of compliance monitoring and evaluation.

Recommendations to implement continuous compliance include:

<table>
<thead>
<tr>
<th>Government</th>
<th>Critical Infrastructure Operators</th>
<th>Continuous Compliance Software Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass legislation to define mandatory cybersecurity standards for critical infrastructure sectors.</td>
<td>Understand regulation standards and educate employees.</td>
<td>Educate critical infrastructure operators on how continuous compliance can help them.</td>
</tr>
<tr>
<td>Increase funding to agencies responsible for cybersecurity (SRMAs and CISA).</td>
<td>Build in security and compliance to development of new products.</td>
<td>Establish institutional knowledge for how to work with small and large businesses.</td>
</tr>
<tr>
<td>Provide funding to small critical infrastructure businesses to adopt continuous compliance.</td>
<td>Grow continuous compliance by stages within a business.</td>
<td>Work with state, local, and tribal governments to promote services.</td>
</tr>
<tr>
<td>Increase financial liability for noncompliance and establish a safe harbor standard.</td>
<td>Self-assess necessary amount of control versus convenience.</td>
<td></td>
</tr>
<tr>
<td>Establish education and promotion programs for continuous compliance.</td>
<td>Segment IT/OT systems to the degree applicable.</td>
<td></td>
</tr>
<tr>
<td>Encourage investment in R&amp;D for AI and automation monitoring.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Critical Infrastructure Regulations in the United States

CISA Critical Infrastructure Sectors

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial base
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Healthcare and public health
- Information technology (IT)
- Nuclear reactors, materials, and waste
- Transportation systems
- Water and wastewater systems

The Cybersecurity and Infrastructure Security Agency (CISA) divides critical infrastructure in the United States into sixteen distinct sectors. These sectors contain facilities ranging from dams and nuclear power plants to sports stadiums and Amtrak stations. They also make up a substantial slice of the US economy and protection of this infrastructure is vital to public safety and national security. Regulatory and compliance standards differ greatly between the sectors; financial service businesses, for example, have numerous regulations to protect customers...
from credit card fraud or avoid nefarious trading practices. These requirements, of course, are substantially different from those regulating the safe disposal of nuclear waste or the functionality of water treatment systems.

Cybersecurity regulations for critical infrastructure, however, are often lacking or simply nonexistent. In fact, the energy, financial, and nuclear industries are the only sectors with mandatory cybersecurity compliance standards. The National Institute of Standards and Technology (NIST)—an agency within the US Department of Commerce without the power to enforce regulations on businesses—publishes a framework that can be used on a voluntarily basis for non-government organizations to improve cybersecurity. While federal government entities are required to adhere to the NIST Framework, businesses are not, though they can use it as a guide to improve cybersecurity. It is a flexible framework that is adaptable to all sixteen critical infrastructure sectors, albeit not enforceable.¹

Despite CISA providing, coordinating, and facilitating cybersecurity advice and knowledge for numerous stakeholders, it is not a regulatory agency and are without enforcement powers in this regard. CISA essentially serves as a conduit for advocating best practices and describing current threats to its government and private sector partners. They have built a reputation as a trusted government partner that seeks to protect and educate but not punish.

In 2013, Presidential Policy Directive 21 defined government agencies that oversee the critical infrastructure sectors as Sector Specific Agencies—now called Sector Risk Management Agencies (SRMAs).² The Department of Energy, partnering with several agencies and organizations—like the North American Energy Reliability Corporation and the Federal Energy Regulatory Commission—regulates the energy sector as one of the few critical infrastructure sectors that has mandatory cybersecurity regulations.³ In 2018, the Department of Energy stood up their Office of Cybersecurity, Energy Security, and Emergency Response

---

to protect the sector from evolving cyber threats.\textsuperscript{4} The energy industry, however, does not operate in a vacuum. Power plants rely on oil and gas, coal, water, nuclear power, and renewables, meaning that disruptions to US energy security could be caused by cyber intrusions at a liquefied natural gas terminal, railway junction, pipeline, or offshore wind turbine—none of which operate under the purview of the Department of Energy. Since energy, like most critical infrastructure sectors, does not operate independently, neither should its security. Vulnerabilities in one sector risk the security of many others. A holistic cybersecurity methodology would prove more robust and effective than the current siloed approach, which neglects the interdependent nature of these sectors.

The March 2022 Cyber Incident Reporting for Critical Infrastructure bill, when it goes into effect following CISA rulemaking, will require businesses to report major cyber incidents within 72 hours and any ransomware payment made within 24 hours.\textsuperscript{5, 6} No reporting requirement previously existed. While this does not add to regulatory requirements to prevent cyber incidents by adding security measures, it ensures that the federal government is aware of ongoing intrusions, allowing for a unified response.

Outside of the 16 defined critical infrastructure sectors, the Federal Risk and Authorization Management Program (FedRAMP) establishes compliance and security standards for cloud service providers that have contracts with the federal government.\textsuperscript{7} Although not defined as critical infrastructure by CISA, cloud service providers are responsible for enormous amounts of data and operational capacity for government clients at the federal, state, local, and tribal levels as well as businesses in both critical infrastructure and non-critical infrastructure sectors.


Compliance Barriers and Challenges

Complying with NIST standards, even though they are voluntary, can be an arduous process. Organizations devote significant financial resources, personnel, and time to monitor and ensure compliance, which can be an expensive and time-consuming endeavor. Extensive and complicated IT networks run by multinational organizations provide ample access points to cyber actors, while limited financial resources and personnel or lack of cybersecurity training present challenges to local utility operators.

Small critical infrastructure operators at the state and local levels may see little value in spending heavily on cybersecurity and compliance teams, which could account for an inordinate portion of their operating costs. Investing in safeguards to meet non-mandatory cybersecurity standards can be a tough sell for under-resourced organizations—particularly for smaller businesses who do not perceive themselves as a target. Many simply do not have the funds, time, or personnel to establish robust compliance practices. Alternatively, they may assess that the cost does not add sufficient value to justify the investment. Regardless of the reason, this leads to security gaps for critical infrastructure operators—and for the public relying on them—in addition to disrupting essential operations in the event of a cyberattack.

---

Security and information assurance standards roughly equivalent to NIST exist outside of the United States. Most prominent is the standard published by the International Organization for Standardization (ISO)—a group in Geneva, Switzerland establishing standards for everything from food safety and child car seats to IT security. ISO has 167 member countries, including the United States. The ISO cybersecurity standard, published jointly with the International Electrotechnical Commission in 2013 and updated for Europe in 2017, is essentially a series of best practices. These, like the NIST Framework, are voluntary for organizations to adopt. While ISO will not perform a certification to verify compliance with its standard, other independent bodies will.

The UK, Germany, and others also publish standards advocating similar security procedures for a variety of companies. Cyber Essentials—the UK version—will even conduct an audit for organizations to determine compliance with their standard. The Cyber Essentials self-assessment, like NIST, can be used by anyone to determine and improve an organization’s cybersecurity posture. A verified assessment costs 300-500 British Pounds and is valid for 12 months. An upgraded bespoke version—Cyber Essentials Plus—is a “hands-on technical verification” that goes deeper to secure one’s IT systems.

Neither ISO nor Cyber Essentials can compel a business to undergo a cybersecurity audit. Even when such an organization does evaluate itself and come into compliance, this only verifies their compliance at the time the assessment was conducted. It is not an ongoing security monitoring service.

What are the current threats to critical infrastructure?

- While there is ample focus on zero-day vulnerabilities in software, most exploitations are some combination of lax security protocols and human error. Even the most secure code, updated with patches regularly, is not immune to determined and sophisticated cyber actors with sufficient knowledge, resources, and time.

- Phishing emails and text messages remain the most effective tactic for infiltrating a network. After years of building cybersecurity awareness and training programs for employees, a well-designed phishing attack can still fool an employee who clicks on a malicious link by mistake.\(^{13}\)

- USB access, lack of multifactor authentication (MFA), leaked credentials available for purchase on the dark web, disgruntled employees, and even former employee credentials that are still active are all other common entry points into otherwise secure networks. Taking basic security steps can prevent most intrusions from these kinds of risk factors. Non-segmented networks—systems that allow an intruder to move around within a network once they gain access through an entry point—are a common risk to companies. Intruders can access a relatively insecure part of a network and then move laterally to more valuable areas, potentially stealing data or accessing operational technology (OT) through IT systems.\(^{14}\)

- Devices used to monitor OT systems are often a vulnerable access point. For example, a sensor monitoring flow rate on remote pipeline likely relies on outdated software that could be decades old. If this sensor is connected to the network, it presents a significant risk unless it is routinely patched or regularly replaced with current operating systems. Devices like these also lack basic cybersecurity requirements.\(^{15}\)

- Regularly patching software when updates are available is an absolute necessity. However, through proper cyber best practices, regular employee training, and other simple measures, organizations can significantly


reduce their attack surface area and limit the number of attackers with the technical sophistication to access their networks.  

**Point-in-time: Compliance in Practice**

Businesses or organizations that do adopt cybersecurity measures must institute some sort of monitoring procedure to ensure that they are adhering to their self-defined standards or best practices. After all, while there may not be a government penalty for noncompliance, it is still painful to experience a cyber incident. Businesses can sustain serious damage to their reputation and bottom line because of a cyberattack. According to Accenture, the average cost of a cybercrime attack in 2018 was $13 million including business disruptions, information loss, revenue loss, and equipment damage.

Many frameworks to ensure compliance with cybersecurity standards are done so on a point-in-time or period-in-time basis, which could be as infrequently as every year. The threat landscape evolves routinely and is reflected in changes to cybersecurity defenses. Regulations, however, seldom adapt quickly. Sectors relying on legislation to mandate cybersecurity compliance, like nuclear and energy, also need to adapt their monitoring mechanisms for new kinds of threats that static regulations will not be adjusted for.

Changes in technology and culture mean that once well-regarded practices are suddenly out of date. For example, with virtual work increasing, the risk to business networks from an employee’s home Wi-Fi connection also increases. Both employee remote access and other third-party access presents a tremendous risk to networks. Businesses that do not provide work computers, phones, or separate wireless connections also have increased danger from these personal device end

---


points. Developing best practices always moves more quickly than regulatory authorities can catch up. When laws are nonexistent or limited, a patchwork of compliance cultures and practices develops, leaving substantial gaps in security.

When businesses prepare for a cybersecurity assessment or audit, they often draw resources from other departments for a significant period. This spike in resource allocation is costly and reduces efficiency in other areas. Despite this immense effort, it still pays to comply with best practices. Globalscape estimated that the cost of cybersecurity compliance for the 53 multinationals it researched was $5.47 million and the cost for non-compliance was $14.82 million.

But given the drain on resources, businesses often fear that additional regulations will hamper their innovative processes and make them less competitive or profitable. Of course, while many businesses do not want burdensome regulations, they understand the benefits of maintaining secure cyber systems. The loss of data from a hack or negative public attention can be bad for revenue. Therefore, many implement their own cybersecurity monitoring and auditing systems, to assess security and risk at specific points in time. The problem with point-in-time compliance is that as soon as the assessment is completed, it is out of date. This method of compliance assessment and auditing relies on observation at a singular point rather than consistent monitoring, making it challenging for an administrator to determine noncompliance at the moment it occurs. Rather, noncompliance may only be detected when someone actually goes and looks for it, allowing for a long dwell time in the event a threat actor embeds themselves undetected in a system to observe network operations. Transitioning from a point-in-time auditing and compliance framework to one that is continuous, agile, and adaptable is necessary it improve cybersecurity for critical infrastructure.

---


Continuous compliance is a security posture and set of operational practices where an organization can persistently monitor, identify, and rectify current or potential lapses in their cybersecurity to ensure adherence to legal standards and industry best practices.\textsuperscript{22} To do so requires a paradigm shift in auditing, assessing, and compliance from point-and period-in-time frameworks to ongoing monitoring, evaluation, learning, and adapting. Technology-based controls for detecting when one’s system begins to drift from the established compliance frameworks allows an organization to get back on track quickly to reestablish security without needing to reallocate resources prior to an audit or assessment. Implementing these procedures and technologies enhances visibility of security systems, reduces the costs of auditing, limits penalties for noncompliance, and improves an organization’s security reputation.

An organization must accomplish three tasks to adopt continuous compliance:

1. **Define and mandate a compliance standard**
   - Required minimal cybersecurity standards like using multi-factor authentication, having data backups, segmentation of OT and IT, replacement of legacy software, and mandatory patching can be defined and monitored.

2. **Establish methods to monitor compliance**
   - Once standards are defined, an organization needs a compliance engine—software and a service that monitors specified inputs to measure compliance, track progress, and identify noncompliant systems and behaviors—to monitor specified metrics.\textsuperscript{23}


Continuous Compliance: Enhancing Cybersecurity for Critical Infrastructure by Strengthening Regulation, Oversight, and Monitoring

3. **Alert administrators and remedy noncompliance**

- When noncompliance is detected—or if systems are drifting away from their compliant state based on the predefined controls—the compliance engine will alert a network administrator, who can take steps to fix it. Compliance metrics should also be updated and adjustable as facts on the ground change. The critical infrastructure sectors must have systems to determine if their networks adhere to new standards that are defined. If something does not meet the new standard, the engine must notify a manager so it can be remedied.

This method of compliance monitoring allows for corrections in real time by identifying noncompliant systems and those that are drifting away from compliance. Compliance in this definition is referring to a range of physical and cyber security practices for both information technology and operational technology systems. The standards can be different across functions or sectors, depending on mandates, guidance, or best practices. The main principles remain though: cybersecurity is not an afterthought to be checked at various points but an ongoing process that is never complete. This is a cultural and institutional shift from viewing compliance as an audit or periodically looking under the hood to make sure everything is running well to a 24/7 monitoring of security so that the current state of cybersecurity can be improved and reported at any time.
There is still a place for audits and point-in-time frameworks. These can be used to produce a report or provide a historical record of compliance. However, because the systems have been monitored continuously, producing these reports, and undergoing an audit will take significantly less manpower and be far cheaper. In preparation of the European Union General Data Protection Regulation (GDPR), forty percent of companies spent over $500,000 to achieve compliance and even more to maintain it.\(^{24}\) However, this figure represents traditional methods for compliance and monitoring. Continuous compliance is not simply auditing more frequently, which would increase costs substantially. Instead, by leveraging software and automation, it allows for a lower, sustained level of investment in compliance and monitoring rather than a spike and resource shift once or twice per year.

Quod Orbis, a cybersecurity company, estimates that by continuously monitoring and complying with set standards, a company can reduce their compliance costs by 75 percent and see a return on investment within five months.\(^{25}\) Furthermore, companies with over 5,000 employees that maintained compliance traditionally spent just $700 per employee.\(^{26}\) So, by complying with best practices, a business reduces cost over noncompliance, and continuous compliance presents a more cost effective, and secure method of doing so.

Many organizations have implemented continuous compliance, but it remains a nascent concept. Implementation in these early adopters has typically involved compliance with privacy laws like GDPR or the California Consumer Privacy Act, but the concept can and should apply to critical infrastructure as well. Any business that needs to adhere to a complicated web of standards and ongoingly monitor hundreds, or thousands, of systems, networks, or devices can benefit from implementing continuous compliance. The advantages of this methodology are that it will not only ensure better cybersecurity—which will reduce the cost of data loss from a hack—but also reduce the costs of audits, which are inherently expensive and time consuming.


Case Study: Colonial Pipeline

On May 7, 2021, hackers accessed and locked nearly 100 gigabytes of data from the Colonial Pipeline Company. Colonial operates a 5,500-mile pipeline from Texas to New Jersey and is the largest pipeline for refined oil products in the United States, carrying up to three million barrels per day. The hackers—later identified as an Eastern European group known as “DarkSide”—demanded a ransom payment in exchange for unlocking and allowing Colonial access to its data.27

The company shut down the pipeline as a precautionary measure despite DarkSide only accessing IT systems and not the company’s OT systems. Colonial later admitted that DarkSide had accessed and restricted their billing system, raising internal concerns that Colonial would be unable to accurately charge its customers for oil consumed.28 This shutdown restricted the supply of 45 percent of fuel for the East Coast until May 12, when the pipeline was reopened. As a result, people began “panic buying” fuel from gas stations, resulting in increased prices at the pump. Airlines adjusted flight schedules because of the fuel shortage and some altered routes or added stops in order to fill up their tanks.29 Colonial paid the ransom of nearly 75 bitcoins ($5 million) to unlock their data.

How could continuous compliance have helped?

To gain access to Colonial’s IT system, DarkSide used a password that had been leaked on the dark web. This password was not set up with MFA.30 They also entered through a legacy Virtual Private Network (VPN) that “shouldn’t have been in use.”31

While all these factors were avoidable using good cyber hygiene techniques and shutting down outdated accounts, they were clearly not visible to Colonial. Colonial either overlooked these vulnerabilities through poor assessment and auditing techniques or did not search for these kinds of risks at all.

A compliance engine would have 1) been able to detect that an account was not set up with MFA, which administrators could have then taken steps to correct; and 2) informed administrators of outdated legacy VPNs that still had access to the network, which could have been removed. In addition to using a compliance engine, if Colonial had employed threat intelligence analysts, they may have been able to identify the leaked password on the dark web prompting an effort to secure that threat vector. With proper data backups, Colonial could also have re-accessed their billing infrastructure quickly and avoided shutting down the pipeline. By mandating cybersecurity requirements for critical infrastructure operators and implementing continuous compliance, this disaster could have been avoided.

**How Continuous Compliance Works**

Technologies and practices—such as Security Information and Event Management—exist to monitor the cybersecurity systems of a business. Compliance engines—like Chef InSpec, AWS Config, or NeQter—are available to provide real-time monitoring and visibility into where a business stands regarding compliance. These engines can, for example, determine whether all employees are using multi-factor authentication in real-time and alert an administrator of those not using it, as opposed to only seeing this during an assessment or audit. These engines are capable of several other tasks including identifying the number of days to deactivate a former employee’s credentials, alerting an administrator when unauthorized entities attempt to access critical systems, or determining whether third party access to networks was cancelled after a project was completed. The engine can determine compliance for other inputs that the administrator defines for it, allowing for a customizable, tailored product for one’s business. A company can require and monitor, for example, if strong security standards—like ensuring encryption keys are 256 bits long or using HTTPS as a default—are used automatically.

Assessing an organization’s risk and security gaps is an important first step in determining areas for improvement. For critical infrastructure operators, it can be an especially powerful tool. When deciding to implement continuous compliance, an organization must successfully map their systems to have a complete visibility

---


in their network. This will allow them to identify weak points and ensure the compliance engine is monitoring all necessary measurements. The engine can identify the number and type of systems with known vulnerabilities so that they can then be patched. It could also monitor data being transferred from the company network. This could indicate that either an outside actor is stealing data, or an employee is downloading it for malign purposes. While a compliance engine is primarily inward looking—as opposed to searching for potential external threats—it ultimately monitors inputs that the company decides.

This provides an opportunity for threat intelligence analysts to work with compliance experts by looking externally. Threat intelligence experts would be able to provide information about what malicious groups are doing, which can then be turned into criteria observed by the compliance engine. For example, a threat intelligence analyst that identified credentials on the dark web could pass that information to those administering the compliance engine to easily check if those credentials were part of the company network. They could also provide lists of known threat actor IP addresses, which the compliance engine could alert managers to if they tried to gain access to the network.

Under-resourced critical infrastructure operators gain further assistance as compliance engines divide certain responsibilities between the organization and the cloud service provider running the compliance engine. For example, the cloud service provider is responsible for security of the cloud service, meaning both network security and physical security of servers and end access points. The client is responsible for security within their use of cloud, including users, applications, firewalls, services, and access management tools. By relying on a cloud service provider, a critical infrastructure operator can reduce certain costs by not building these tools in-house. It will also have the added benefit of the enhanced security by relying on a business that does this full time, which is especially important for small businesses. Both the provider and client can work together to map the network and identify what standards and metrics should be monitored. The organization itself will have the most awareness of its own systems and networks, which can then be paired with the software offered by the cloud service provider.

The critical infrastructure operator is also responsible for the security of operational technology it manages. While adoption of continuous compliance requires a cultural shift, it also requires certain technologies, such as those employing automation and machine learning, to be fully effective. OT that is network-connected must also be monitored and patchable, otherwise it presents an enormous security risk.

Automation is an absolute necessity to build effective continuous compliance methods. Advancements in artificial intelligence (AI) will help increase automation speeds and make continuous compliance more efficient. Current methods of compliance are slow, expensive, and ineffective. With AI, continuous compliance will be more efficient and capable of scaling effectively.

Building in security and compliance from the beginning into software development and IT operations allows an organization to roll out new applications quickly, securely, and in a cost-effective manner. Instead of adding security as an additional layer at the end of verifying a program, adopting an agile mindset to security and development can increase scalability, efficiency, and profitability.
Case Study: Oldsmar, Florida Water Treatment Facility

On February 5, 2021, a hacker accessed a computer at the water treatment plant serving Oldsmar, FL—a city near Tampa with a population of about 15,000. The hacker increased the level of sodium hydroxide from 100 parts per million (ppm) to 11,100 ppm, which is a toxic and deadly amount for humans to ingest. Luckily, an employee noticed the increase and reduced the levels back to normal before the chemicals entered the water supply.35

The Oldsmar water treatment plant is a small, municipal facility with a limited staff and without a lot of funding. They were using a remote access service, called TeamViewer, so that employees could monitor and alter the levels of chemicals in the water without being physically at the facility. The hacker used TeamViewer to login into the system remotely and change the chemical levels.36 The facility, however, used the same password for their remote access accounts rather than individuals each having a separate one.37 This made it incredibly easy for the hacker to access the system. The Oldsmar facility had stopped using TeamViewer but had not uninstalled it or prohibited access. In addition to not segmenting IT and OT systems, Oldsmar was still using Windows 7, for which Microsoft no longer provided updates.38

How could continuous compliance have helped?

Ultimately, the Oldsmar example highlights the impact of the dearth of cybersecurity regulations for water treatment facilities, minimal funding, and limited cybersecurity practices and training of employees.

With mandatory cybersecurity standards and continuous monitoring and compliance, all the factors that allowed a hacker to access Oldsmar’s water treatment facility so easily would have been avoidable. For example, a compliance engine would have alerted administrators that Windows 7 was no longer being patched, that TeamViewer still had access to the network even though it was no longer in use, and that employees were not using MFA or even different credentials.
It is understandable that such a small treatment facility may not have resources to invest in a compliance engine of their own, but other strategies exist. Small utilities should consider pooling resources with others in the area, or they could piggy-back off a large, nearby city, like Tampa, with more resources to invest in security services. Additional funding from either the state or federal government in addition to required cyber standards could prevent further incidents like this one. The people of Oldsmar were fortunate that the employee noticed the change in chemical levels and acted in time, the next city might not be so fortunate.
Recommendations

The following recommendations can begin moving critical infrastructure towards using continuous compliance. They fall into three broad categories: government action and investment, critical infrastructure operator adoption and education, and continuous compliance provider implementation.

Government

1. Pass legislation to define mandatory cybersecurity standards for critical infrastructure sectors

- It is impossible to continuously comply with a standard if those standards are not clearly stated. This recommendation would work to define those standards and make them compulsory and to protect SRMAs from future Supreme Court rulings that undercut the ability of executive agencies to regulate.\(^\text{39}\) Each SRMA should enforce the regulations for their respective critical infrastructure sector. Because the sixteen sectors operate so differently, each SRMA should establish an advisory board to work with companies in their corresponding businesses to create rules tailored to each sector. The legislation must reflect that security be built into a network’s development and not simply layered on top of existing systems. Regulations that produce “box checking” behavior result in subpar cybersecurity. By including security within the development of networks and applications—and then requiring ongoing monitoring requirements—businesses can begin to transition towards a continuous compliance framework.

- SRMAs should spot-check to verify that critical infrastructure organizations are compliant, but the onus must be on the company management to stay in compliance with the standard. The standard, however, for each sector should emphasize continuous monitoring rather than reflect a point-in-time framework. Therefore, companies must be able to establish continuous compliance frameworks.

2. **Increase funding to SRMAs and CISA**

- Each SRMA should have more resources to better monitor compliance for their respective sector. With the additional rules stated in the above recommendation, the agencies responsible for enforcing those rules must have the resources to ensure proper adherence. Laws without enforcement mechanisms results in chaos. A robust enforcement capability paired with the non-enforcement assistance from CISA will help companies get compliant and stay compliant.

3. **Provide funding to small critical infrastructure businesses to adopt continuous compliance**

- Large corporations in sectors like energy, finance, and defense can devote sufficient funds to meet new guidelines. They can hire personnel to monitor compliance, contract with cloud service providers, and install new software and hardware for monitoring. Some small critical infrastructure companies, however, in sectors like food and agriculture, or water and wastewater, may struggle to devote the necessary capital to ensure compliance with new standards. They must be provided with funds to upgrade hardware and software, institute new procedures, and train existing employees.

- As part of the Bipartisan Infrastructure Bill, the US Congress authorized $1 billion over four years for critical infrastructure cybersecurity, most of it going to state, local and tribal governments. Another $250 million from the bill is going to cybersecurity for rural and municipally owned energy utilities, which will be used to bolster cyber defenses and increase threat information sharing. Another $350 million is provided for increasing cybersecurity defenses and monitoring for the Department of Energy.40 These investments are critical and should be continued. However, more funding needs to be provided for all small utilities to help implement new compliance standards. It was costly for businesses to adopt GDPR standards and it will take an initial cost to implement these too.

---

• This investment on the front end will allow smaller businesses to use automation tools to better monitor compliance at a lower cost than they currently do on a point-in-time basis. Allowing smaller utilities to lag behind will just extend already existing security gaps. Lowering costs for these businesses can also be furthered by pooling monitoring and compliance operations amongst multiple facilities, especially in rural areas.

4. **Increase financial liability for noncompliance and establish a safe harbor standard**

• As part of the additional regulations, critical infrastructure companies should be held liable for breaches that happen to their networks that either contained vulnerabilities for which patches existed or for lax security that was noncompliant. These companies should be held financially liable or criminally liable if personal harm is done. Businesses will, of course, buy cyber insurance. The insurers will act as an additional check on compliance to the government. Cyber insurance companies will either refuse to cover organizations that are careless, or they will charge them exorbitant rates, motivating the business to simply comply with insurance standards. Furthermore, providing a carrot for businesses that do adhere to published standards and best practices by establishing a safe harbor law will encourage them to improve security. If an organization is compliant and continuously monitoring their security so compliance can be verified, they should be free from liability unless they are negligent. This could save companies millions of dollars, motivating them to stay within the boundaries set by the SRMA.

5. **Establish education and promotion programs for continuous compliance**

• In addition to the valuable work that CISA already does in working with critical infrastructure operators, the agency should conduct a feasibility study on nascent methods like continuous compliance and host roundtables to discuss challenges and opportunities. Furthermore, in passing legislation mandating cybersecurity requirements, CISA and the SRMAs should help smaller utilities understand best practices and opportunities for continuous compliance during the grace period before regulations are enforced. These programs can help businesses understand efficient ways of complying with the new standards passed.
6. **Encourage investment in R&D for AI and automation monitoring**

- The exponential speed of computing and automation in the coming decades will allow continuous compliance to move to a reality for all critical infrastructure sectors. Investments today to speed the process along and maintain a competitive advantage will ensure critical infrastructure security can stay ahead of the growth curve. Automation is critical for continuous compliance to be efficient and cost effective. Without robust automation and machine learning, continuous compliance cannot work. Government should work with the private sector to find opportunities for investment in and promote promising technologies.

**Critical Infrastructure Operators**

1. **Understand regulation standards and educate employees**

- Critical infrastructure operators will have to understand the new regulations and what it means for their organizations. They will also need to work with their SRMA to codify the specific regulations for their sector. Following these steps, each operator must determine how they can implement the new regulations and educate their employees through additional training on the standards and best practices.

2. **Build in security and compliance to development of new products**

- To be competitive, businesses often want to churn out a new product when it is ready and can iterate to make improvements—especially in the tech world. However, this allows for security lapses and breaches in compliance. Integrating security and compliance engineers into the development stage of new products is part of continuous compliance to make sure that products are secure at the time they become operational.41

3. **Grow continuous compliance by stages within a business**

- Organizations can begin piloting continuous compliance with a single entity within their company to help drive cultural change. Making a small investment to achieve this will demonstrate its usefulness and cost saving...
measures, which can then be expanded into other business units and eventually to the entire organization. Automation is far easier to scale than non-automated, human-run systems. So, after a piloting phase, a business can make the transition to continuous compliance quickly.

4. **Self-assess necessary amount of control versus convenience**

   - Businesses, most of which will need to use a cloud service provider to implement continuous compliance, should determine their level of comfort in the tradeoff between control and convenience. Companies that prefer complete control can opt for self-managed tools that allow them full use with little reliance on outside firms. Others may select a managed compliance engine, which allows for greater cost sharing and convenience but sacrifices a degree of command.

5. **Segment IT/OT systems to the degree applicable**

   - While this is not always possible for some businesses, if they are able to separate IT systems, which can be used to access OT systems, then a data breach will not result in a shutdown of the facility. For example, if data is compromised at a nuclear power plant but the reactor can still produce energy, this is much less of a problem than if the hacker can navigate from the payroll system to the reactor operations. Businesses must adopt these practices on their own, but compliance engines can help detect when there are systems not following these guidelines and alert an administrator—avoiding a potential catastrophe.

**Continuous Compliance Software Providers**

1. **Educate critical infrastructure operators on how continuous compliance can help them**

   - The critical infrastructure sectors may view new regulations as burdensome and express frustration with the investments they will have to make. Continuous compliance providers should conduct outreach to these businesses to help them understand that a more efficient, secure, and cost-effective option exists. Each sector is different, and each business is different, so continuous compliance service providers will need to learn
about how the different sectors operate and what regulations they need to follow.

2. **Establish institutional knowledge for how to work with small and large businesses**

   - Selling to large, wealthy companies will be entirely different from small, rural utilities. Continuous compliance service providers should work with these companies to identify their needs and tailor their products to meet them. These providers should also identify ways to pool compliance resources amongst several small utilities. Despite continuous compliance being cheaper than point-in-time compliance, these small utilities will still see an initial cost to meet new regulations. By allowing pooled compliance frameworks, continuous compliance providers can help reduce this cost even further. However, segmentation of networks should still be required to reduce the risk of lateral movement between different critical infrastructure operators in the event of a breach.

3. **Work with state, local, and tribal governments to promote services**

   - Continuous compliance providers should not only reach out to critical infrastructure operators but also the government entities that oversee them. Many small providers will have a closer relationship with state government than federal government. Establishing contacts with local enforcement agencies and offering a potential solution that will save money for state critical infrastructure operators is a good strategy to promote their services. This will also expand the reach of continuous compliance providers to smaller and more secluded critical infrastructure operators.
Conclusion

The current cybersecurity regulatory framework for the sixteen critical infrastructure sectors is fragmented and minimal. Many sectors have few, or no, regulations regarding cybersecurity. Cyberattacks—whether from a ransomware group, nation-state, or disgruntled employee—risk personal information and data as well as physical operations with real-world consequences. When critical infrastructure is concerned, these impacts can do enormous damage to the economy and risk public safety. Regulation is necessary to motivate sectors to take cyber threats seriously and provide companies the necessary tools to improve their security, detection, and attack mitigation practices.

The physical security of important, and frequently targeted, sites is not done on an intermittent basis. It is ongoing and routinely monitored. Cybersecurity for such sites should be too. Continuously monitoring and ensuring adherence to a published, well-defined, and agreed upon standard is a must to establish safe and reliable critical infrastructure providers that citizens can have faith in functioning when they need them to (which is always). Shifting one’s security and compliance mindset from periodically checking in to see if standards are met, and then reestablishing compliance if they are not, is no longer feasible.

Knowing that one complies with a standard should be the norm and when a system is noncompliant, it should be an anomaly in which resources are immediately dedicated to getting back on track. Detecting drift from the agreed upon standard before a system violates compliance rules and allowing an administrator to take corrective actions can preempt potentially vulnerable systems and facilities.

AI, machine learning, and automation will make this monitoring easier, faster, and more holistic as the technology advances. Legislation that defines standards open to technological progress must be implemented to provide guardrails as AI and machine learning advance the speed and power of devices. These regulations must be adjusted as technological advancements render moot the current rules. Automation is a crucial component to making continuous compliance feasible and scalable. As the enabling technologies continue to advance, continuous compliance can become even less resource intensive and more effective.
These procedures and standards need to be built into the fabric of a business to institute the cultural changes necessary. By working with government to make smart, achievable cybersecurity standards, and implementing continuous compliance frameworks, businesses can ensure that critical infrastructure is safe, reliable, and affordable.